(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 November 2001 (08.11.2001)

PCT

(10) International Publication Number
WO 01/84765 A2

(51) International Patent Classification[7]: H04L 7/00

(21) International Application Number: PCT/EP01/04686

(22) International Filing Date: 25 April 2001 (25.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/562,682 2 May 2000 (02.05.2000) US

(71) Applicant: TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: BASILIER, Henrik; Apt. #1823, 2643 Old Quarry Rd., San Diego, CA 92108 (US). GUSTAFSON, Ulf; 201 Harrison, San Francisco, CA 94105 (US).

(74) Agents: FÜCHSLE, Klaus et al.; Hoffman . Eitle, Arabellastrasse 4, 81925 München (DE).

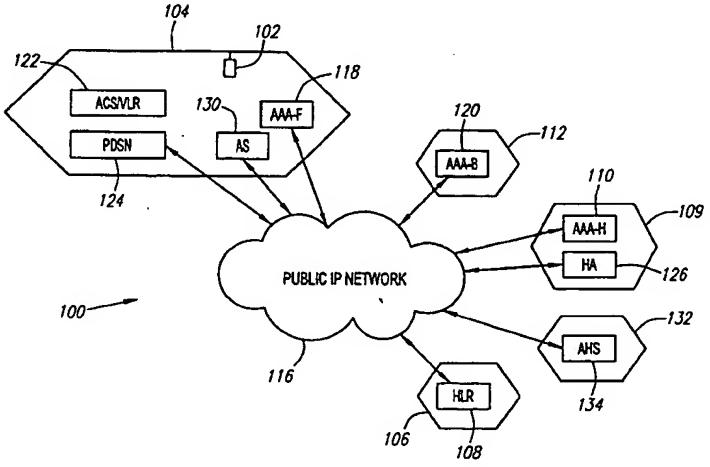
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR COMBINED TRANSMISSION OF ACCESS SPECIFIC, ACCESS INDEPENDENT AND APPLICATION SPECIFIC INFORMATION OVER PUBLIC IP NETWORKS BETWEEN VISITING AND HOME NETWORKS



(57) Abstract: A method and system for transmitting specific information, such as access specific roaming information and/or application specific information, between a home network and a visiting access network is provided. The home network and visiting network are capable of communicating access independent information in a protocol, such as a AAA protocol. The access and/or application specific information is formatted in the AAA protocol. The access and/or application specific information is then transmitted over a public IP network between the home network and the visiting network. A system is provided for transmitting access and/or application information between a visiting network and a home network over a public IP network. A control access server in the visiting access network formats the access information using a secure AAA protocol to form formatted access information. An application server formats application specific information. A AAA-F server associated with the visiting network transmits the formatted access and/or application information over the public IP network to the home network.

WO 01/84765 A2

Method and System for Combined Transmission of Access Specific, Access Independent and Application Specific Information Over Public IP Networks Between Visiting and Home Networks

Background of the Invention

The present invention relates generally to methods and systems for providing roaming among communications systems, and more particularly, to a method and system for transmitting access specific and/or application specific information from a visiting access network to a home network using public internet protocol networks.

A variety of wireless mobile communication systems now cover a large portion of the world's surface. Such an expansive coverage is accomplished by a number of different networks operating in specific locations throughout the world. These multiple networks unfortunately also have multiple access types. In order to service users while traveling, or roaming, in other networks, service providers have had to develop methods for providing service to their subscribers while in other networks.

One method for handling the problem of multiple access types is to provide an architecture for separating access specific aspects of roaming from the access independent aspects of roaming. One such architecture has been defined in cdma2000 wherein terminal equipment is authenticated through an access specific means and user registration is accomplished through an access independent means.

In current methods, the two access means are physically separated in the architecture. In the above example, the terminal equipment authentication is performed using specific protocols over the public switched telephone network (PSTN) or a private (protected) network. Security is therefore enforced by isolating the communication path from unauthorized access.

The user conversely is typically authenticated using internet protocol (IP) based protocols running over a shared public IP network. For example, a user will typically have a home IP network from which service is provided. When roaming to other networks, or "visited access networks", the user may still want to receive service. The visited access network contains a function called AAA-F. The AAA-F stores information about roaming partners and/or available brokers. The home network contains a function designated AAA-H which has a database of all subscribers and performs the authentication of a user.

Between the home network and a visited access network a number of broker functions, designated AAA-B, may be present. Access independent information is typically transmitted between the AAA functions over a public IP network. These

transmissions are secured by the use of shared secrets and encryption and eventually a Public Key Infrastructure.

Unfortunately, the use of PSTN networks and private networks increases costs for service providers and reduces the scalability of their systems. Accordingly, there is a need for a method and system which does not use PSTN or private networks to carry signaling information for roaming, which employs public IP networks to transmit access specific and/or application specific information between networks and which transmits the access specific and/or application specific information using available protocols.

Summary of the Invention

This need is met by the method and system of the present invention in which specific information, which may be access specific and/or application specific information is transmitted between visiting and home networks using public IP networks.

In accordance with one aspect of the present invention, a method for transmitting specific information between a home network and a visiting access network is provided. Specific information may comprise access specific roaming information and/or application specific information. The home network and visiting access network are capable of communicating access independent roaming information in a protocol, such as a AAA protocol with AAA encryption. The specific information is formatted in the protocol. The specific information is then transmitted over a public IP network between the home network and the visiting network.

The specific information may be registration or authentication information. The AAA protocol may be a DIAMETER protocol. The step of formatting the specific information in a AAA protocol may comprise the step of encrypting the specific information at an access control server in the visiting network. Alternatively, for application specific information, encryption may be performed by an application server. The method may comprises the steps of transmitting the encrypted specific information from the visiting network to the home network and decrypting the encrypted specific information at the home network. Depending upon the relationship between the visiting network and the home network, the formatted specific information may be transmitted to a broker AAA server. The broker AAA server then routes the formatted specific information to a HLR for access specific information, or to a application home server for application specific information, based on routing information in the broker AAA server.

In accordance with another aspect of the present invention, a method for providing access specific and access independent roaming capabilities between a home access network and a visiting access network is provided. The method comprising the steps of encrypting the access specific information in a secure protocol at an access control server

in the visiting access network to form formatted access specific information; providing the formatted access specific information to an AAA-F server associated with the visiting access network; transmitting the formatted access specific information to the home access network over a public IP network and decrypting the access specific information at the home access network.

In accordance with another aspect of the present invention, a method is provided for transmitting application specific information between a visiting network and a home network. The home network and visiting network are capable of communicating access independent roaming information in a protocol, such as a AAA protocol with AAA encryption. The application specific information is formatted in the protocol. The application specific information is then transmitted over a public IP network between the home network and the visiting network.

In accordance with yet another aspect of the present invention, a system for transmitting specific information, such as access specific roaming information and/or application specific information, between a visiting network and a home network over a public IP network is provided. The system includes a server associated with the visiting network for formatting the specific information using a secure AAA protocol to form formatted specific information. A AAA-F server associated with the visiting network transmits the formatted specific information over the public IP network to the home network.

The system may further comprise a HLR server associated with the home network for receiving formatted access specific information and for providing the formatted specific information to the home network. A broker network may receive the formatted specific information from the public IP network and route the formatted specific information over the public IP network to the home network. The access control server may provide an international mobile subscriber identity in the access specific information which identifies the AAA-H server.

These and other features and advantages of the present invention will become apparent from the following detailed description, the accompanying drawings and the appended claims.

Brief Description of the Drawings

The foregoing and other advantages of the invention will become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 is schematic diagram of a system in accordance with the present invention including AAA-F and AAA-H servers which are used to communicate access specific,

access independent and application specific information over public IP networks between a visited network and a home network;

FIG. 2 is a graphical representation of message transmission between various components of the system shown in FIG. 1; and

FIG. 3 is a graphical representation of a message format which may be advantageously employed in accordance with the present invention.

Detailed Description of the Invention

A system 100 which uses public IP networks to communicate access specific, access independent and application specific information as a user, or mobile terminal 102, roams in a visited access network 104 in accordance with the present invention is shown in FIG. 1. A home access network 106, such as a cdma2000 network, provides wireless service to the user 102. As is known, the home access network 106 is associated with a Home Locator Register (HLR) 108 which stores information relating to subscribers of the network service which is used to identify and verify subscribers. The HLR 108 also stores information regarding features and services subscribed to by each subscriber. A home IP network 109 has an associated Authentication, Authorization and Accounting (AAA-H) function 110.

A broker network 112 is shown connected to a public IP network 116. As will be apparent to those skilled in the art, a broker network may or may not be needed to provide service to the mobile terminal 102 depending upon the relationship between the home access network 106 and the visited access network 104. The public IP network 116 supports communications between the various components of the system 100 as discussed more fully below.

Similar to the AAA-H function 110, the visited access network 104 and the broker network 112 are associated with a AAA-F function 118 and a AAA-B function 120, respectively. The various AAA functions communicate with each other using an appropriate encryption method (AAA protocol encryption) and a specified AAA protocol format.

In addition, the visited access network 104 contains an access control server/visitors' location register (ACS/VLR) 122 which requests information from the HLR 108 and stores that information as long as the mobile terminal 102 is roaming in the visited network 104. A packet data serving node (PDSN) 124 in the visited access network 104 supports packet communications. A home agent (HA) 126 in the home IP network 109 provides mobile IP based packet data services to the mobile terminal 102. Both the PDSN 124 and the HA 126 are known in the art and, as such, details of their operation will be not given herein.

In accordance with the present invention, application specific information may be transmitted over the public IP network 116. An application server (AS) 130 is provided in the visited network 104 for transmitting, encrypting and receiving application information. An application home network 132 contains an application home server (AHS) 134 which stores and provides information relating to applications subscribed to by the user. Although the discussion below will be directed primarily to the transmission of access specific information, the application specific information may be transmitted in a similar manner similar in accordance with the present invention.

The specific configuration of the system 100 shown in FIG. 1 is exemplary and may take many other forms. For example, many of the components may be included, or part of, other components. The AAA-F 118, the AAA-H 110 and/or the AAA-B 120 may be stored on a single server. Further, the home IP network 109 and the public IP network 116 may be a single IP network or be part of the home access network 106. In addition, numerous communications paths between the various components of the system 100 have not been shown for clarity and ease of description.

The present invention advantageously uses, to a large extent, the framework built for access independent roaming. This is done by running access specific (and/or application specific) protocols for roaming on top of the generic access independent solutions already in place. An example from the wireless world would be to run for example mobile application part (MAP) or American National Standards Institute standard 41 (ANSI-41) on top of the AAA protocol. The AAA protocol may be a known DIAMETER protocol.

Advantageously, in accordance with an aspect of the present invention, the access specific part in both the visited access network and the home access network communicate with the AAA-F using a shared public IP network and the AAA protocol. Thus, the protocol implementations and AAA mechanisms which are currently used for the access independent portions may be reused for access specific portions in accordance with the present invention. Existing access independent roaming agreements may be also reused for access specific roaming with the proper reconfiguration of the AAA servers 118, 120 and 110.

With reference to FIG. 2, exemplary operation in accordance with the present invention will now be described. For this example, the mobile terminal 102 is a code division multiple access (CDMA) terminal and the networks 104 and 106 are respectively a visited cdma2000 network and a home cdma200 network. A user wishes to use the mobile terminal 102 in the visited cdma2000 network 104 which has a roaming agreement with the home cdma2000 network 106. In addition, the AAA-F 118 contains routing information relating to the mobile terminal 102. In initiating communications, the mobile

terminal 102 registers in the visited network 104 by any proper means, such as power up, implicit, or the like.

The ACS/VLR 122 assembles an ANSI-41 registration, and/or authentication, message in an AAA protocol format with AAA protocol encryption. The ACS/VLR 122 then sends the formatted registration message to the AAA-F 118. Using a Network Access Indicator (NAI) field of the AAA protocol, the AAA-F 118 routes the formatted registration message to the HLR 108 associated with the mobile terminal 102. Advantageously, in accordance with the present invention, the access specific roaming information (the registration message) is sent over a public IP network, such as the network 116. The HLR 108 employs a similar process in responding to the received registration message. In effect, the HLR 108 either validates or denies the registration request.

In responding to the received registration message, the registration message is sent to the HLR 108. The HLR 108 decrypts and deciphers the message and either validates or denies the registration request. The HLR 108 generates an appropriate response message which is formatted in the AAA protocol including the AAA protocol encryption. The encrypted response message is transmitted over the public IP network 116 to the visited access network 104. The encrypted response message is routed to the AAA-F 118 server which routes the encrypted message to the ACS/VLR 122 where the response message is decrypted. Based on the response message content, the visiting access network 104 either provides service to the mobile terminal 102 or denies service.

In a second example, the mobile terminal 102 is in the visited network 104 which has a roaming agreement with the home network 106, however, in this situation, routing information for the mobile terminal 102 is not contained in the AAA-F 118. The mobile terminal 102 initially registers in the visited network 104 by any appropriate means. The ACS/VLR 122 assembles an ANSI-41 registration, and/or authentication, message in the AAA protocol format with AAA protocol encryption. The formatted and encrypted registration message is sent to the AAA-F 118. Using the NAI field of the AAA protocol, the AAA-F 118 routes the registration message to an AAA-B, such as the AAA-B 120, which contains routing information for the HLR 108 of the mobile terminal 102. Based on this routing information, the AAA-B 120 routes the registration message to the HLR 118. The HLR 118 validates or denies the registration request using a similar process. Alternatively, the AAA-B 120 may act as a type of redirect server and provide instructions to the AAA-F 118 how to forward the message.

The AAA protocol, for example DIAMETER, is typically built up in a very transparent way, focusing on a reliable transport, as well as hop-by-hop and/or end-to-end security. A typical layout of a message 300 in the AAA protocol is shown in FIG. 3. The

message 300 contains an Internet Protocol (IP) header 302 which is used to route the message 300 between the AAA servers 118, 120 and 110. A user datagram protocol/transmission control protocol (UDP/TCP) header 304 may be provided next to the IP header 302. A AAA header 306 contains information used for routing of the message 300 between the various AAA servers, such as AAA servers 118, 120 and 110. An example of the AAA header 306, or such an information field, is the Network Access Identifier (NAI), as specified by the Internet Engineering Task Force (IETF).

A AAA payload 108 typically carries a registration/authentication message to be used for access authentication. Alternatively, in accordance with the present invention, application specific information may be carried in the AAA payload 308. The AAA payload 308 could, for example, contain messages inherited from MAP/ANSI-41. Encryption may be applied to the AAA payload 308 and/or to the AAA header 306. The encryption applied to the AAA payload 308 would be end-to-end encryption while encryption applied to the AAA header 306 would be hop-by-hop encryption, whereby each AAA server decrypts the AAA header 306 field.

It should be noted that for appropriate routing of the message 300, a NAI has to be constructed by the ACS/VLR 122. The construction of the NAI must be done so that the network 109 of the home access provider (the home network 106) may be found through established roaming agreements. One method may be to use an International Mobile Subscriber Identity (IMSI). Using the IETF syntax of NAI, the format could for example be:

<Significant digits of IMSI>@wirelessdomain.net

The significant digits of IMSI are the digits needed to uniquely identify a HLR and/or a wireless provider. The wirelessdomain.net could be a domain name jointly used by a set of roaming wireless access providers. This domain name could be used to point out the broker AAA server administrating the roaming agreements.

For the example given above wherein the AAA-F 118 contains roaming information regarding the mobile terminal 102, the AAA-F 118 would analyze the received IMSI digits in the NAI and though internal tables locate the appropriate AAA-H 110. For the example wherein the AAA-F 118 did not contain roaming information for the mobile terminal 102, the AAA-F 118 would only need to conclude using internal tables that a specific AAA-B has to be used. The specific AAA-B would be identified based on wirelessdomain.net.

In another aspect of the present invention, application specific information is transmitted over the public IP network 116 using the existing AAA protocol infrastructure. Users subscribe to different applications. For example, some users may subscribe to voice over IP service while others do not. Internet service providers (ISPs) or the like therefore

need to authenticate a user before providing specific applications, or services, to the user. In accordance with an aspect of the present invention, the application specific authentication information may be transmitted from the user to the application home network 132 using a process similar to that discussed above.

For purposes of application specific information, the AS 130 communicates using the AAA network (AAA-F 118 and AAA-B 120) and the public IP network 116 with the application home network 132 and more particularly, the AHS 134. Application specific information, such as authentication information, is assembled in an AAA protocol format with AAA protocol encryption by the AS 130. The AS 130 then transmits the encrypted application specific data to the AAA-F 118 in the visiting access network 104. The application specific information may be formatted as described above with respect to access specific information. The AAA-F 118 transmits the encrypted application specific information over the public IP network 116 to one or more AAA-B 120, if necessary, then to the AHS 134. The AHS 134 validates or denies the authentication request for an application using a similar process.

While the invention may be susceptible to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and have been described in detail herein. However, it should be understood that the invention is not intended to be limited to the particular forms disclosed. Rather, the invention is to cover all modification, equivalents and alternatives falling within the spirit and scope of the invention as defined by the following appended claims.

Claims

1. A method for transmitting specific information between a home network and a visiting access network, the home network and visiting access network being capable of communicating access independent roaming information in a protocol, the method comprising the steps of:

formatting the specific information in the protocol; and

transmitting the specific information over a public IP network between the home network and the visiting access network.

2. The method as recited in claim 1 wherein the step of formatting the specific information in the protocol comprises the step of:

formatting application specific information in the protocol.

3. The method as recited in claim 1 wherein the step of formatting the specific information in the protocol comprises the step of:

formatting access specific roaming information in the protocol.

4. The method as recited in claim 3 wherein the step of formatting the access specific roaming information comprises the step of:

formatting the access specific roaming information in a AAA protocol.

5. The method as recited in claim 4 wherein the step of formatting the access specific roaming information in a AAA protocol comprises the step of:

formatting the access specific roaming information in accordance with Mobile Application Part standards.

6. The method as recited in claim 4 wherein the step of formatting the access specific roaming information in a AAA protocol comprises the step of:

formatting the access specific roaming information in accordance with American National Standards Institute 41.

7. The method as recited in claim 4 wherein step of formatting the access specific roaming information in the protocol comprises the step of:

formatting registration information in the AAA protocol.

8. The method as recited in claim 4 wherein step of formatting the access specific roaming information in the protocol comprises the step of:

formatting authentication information in the AAA protocol.

9. The method as recited in claim 4 wherein the step of formatting the access specific roaming information in a AAA protocol comprises the step of:

formatting the access specific roaming information in accordance with a DIAMETER protocol.

10. The method as recited in claim 4 wherein the step of formatting the access specific roaming information in a AAA protocol comprises the step of:

encrypting the access specific roaming information at an access control server.

11. The method as recited in claim 10 further comprising the step of:

transmitting the encrypted access specific roaming information from the access control server to an AAA server;

routing the encrypted access specific roaming information to a home location register in the home access network; and

decrypting the encrypted access specific roaming information in the home location register.

12. The method as recited in claim 4 wherein the step of transmitting comprises the steps of:

transmitting the formatted access specific information to a broker AAA server; and

routing the formatted access specific information to the home access network based on routing information in the broker AAA server.

13. A method for providing access specific and access independent roaming capabilities between a host access network and a visiting access network comprising the steps of:

encrypting the access specific information in a secure protocol at a access control server in the visiting access network to form formatted access specific information;

providing the formatted access specific information to an AAA-F server associated with the visiting access network;

transmitting the formatted access specific information to the home access network over a public IP network.

14. The method as recited in claim 13 wherein the step of encrypting the access specific information in a secure protocol comprises the step of:

encrypting the access specific information in a AAA protocol with AAA encryption.

15. The method as recited in claim 13 wherein the step of transmitting the formatted access specific information to the home access network over a public IP network comprises the steps of:

transmitting the access specific information to a broker network over the public IP network; and

transmitting the access specific information from the broker network to the home access network based on routing information obtained from a AAA-B server associated with the broker network.

16. The method as recited in claim 13 wherein the step of providing access specific information from the visiting access network to an AAA-F server associated with the visiting access network comprises the step of:

providing AAA server information identifying the AAA-H server associated with the home access network in the access specific information.

17. The method as recited in claim 16 wherein the step of providing AAA server information identifying the AAA-H server associated with the home access network in the access specific information comprises the step of:

providing an international mobile subscriber identity in the access specific information.

18. The method as recited in claim 13 wherein the step of providing access specific information from the visiting access network to an AAA-F server associated with the visiting access network comprises the step of

providing registration information in the access specific information.

19. A system for transmitting access specific information between a visiting access network and a home access network over a public IP network comprising:

a control access server in the visiting access network for formatting the access specific information using a secure AAA protocol to form formatted access specific information; and

a AAA-F server associated with the visiting access network transmitting the formatted access specific information over the public IP network to the home access network.

20. The system as recited in claim 19 further comprising:

a broker network for receiving the formatted access specific information from the public IP network and for routing the formatted access specific information over the public IP network to the home access network.

21. The system as recited in claim 20 wherein the access control server provides an international mobile subscriber identity in the access specific information which identifies the home access network.

22. A method for transmitting application specific information between a visiting network and a home network, the home network and visiting network being capable of communicating access independent roaming information in a protocol, the method comprising the steps of.

formatting the application specific information in the protocol; and

transmitting the application specific information over a public IP network between the home network and the visiting network.

23. The method as recited in claim 22 wherein the step of formatting the application specific information in the protocol comprises the step of:

formatting the application specific information in a AAA protocol.

24. The method as recited in claim 23 wherein the step of formatting the application specific information in a AAA protocol comprises the step of:

formatting the application specific information in accordance with Mobile Application Part standards.

25. The method as recited in claim 23 wherein the step of formatting the application specific information in a AAA protocol comprises the step of:

formatting the application specific information in accordance with American National Standards Institute 41.

26. The method as recited in claim 23 wherein step of formatting the application specific information in the protocol comprises the step of:

formatting authentication information in the AAA protocol.

27. The method as recited in claim 23 wherein the step of formatting the application specific information in a AAA protocol comprises the step of:

formatting the application specific information in accordance with a DIAMETER protocol.

28. The method as recited in claim 23 wherein the step of formatting the application specific information in a AAA protocol comprises the step of:

encrypting the application specific information at an application server.

29. The method as recited in claim 23 wherein the step of transmitting comprises the steps of:

transmitting the formatted application specific information to a broker AAA server; and

routing the formatted application specific information to the home network.

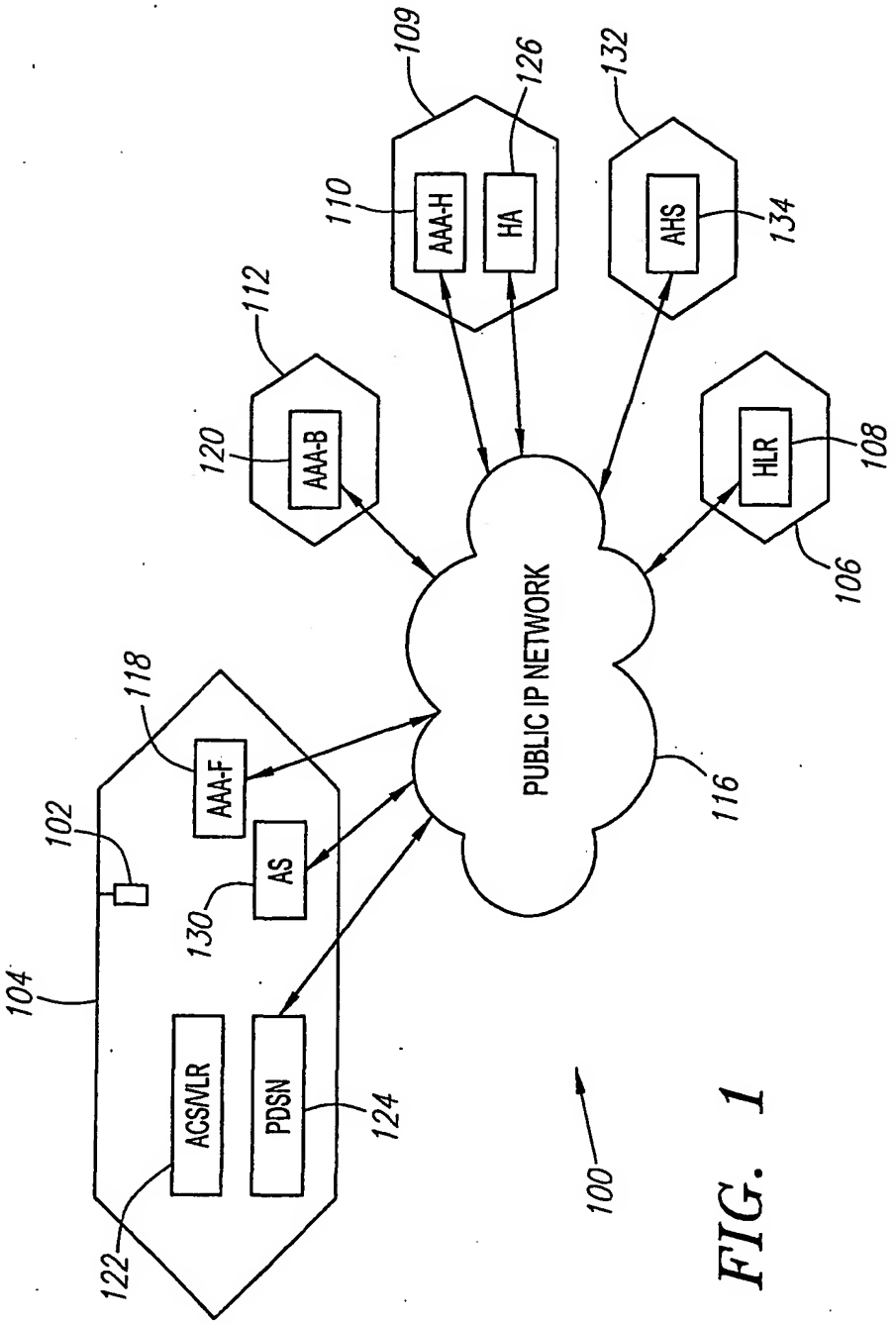

109
126
132
110
AAA-H
HA
AHS
134
112
120
AAA-B
HLR
108
106
PUBLIC IP NETWORK
116
118
AAA-F
102
AS
130
104
ACS/MLR
PDSN
124
122
100

FIG. 1

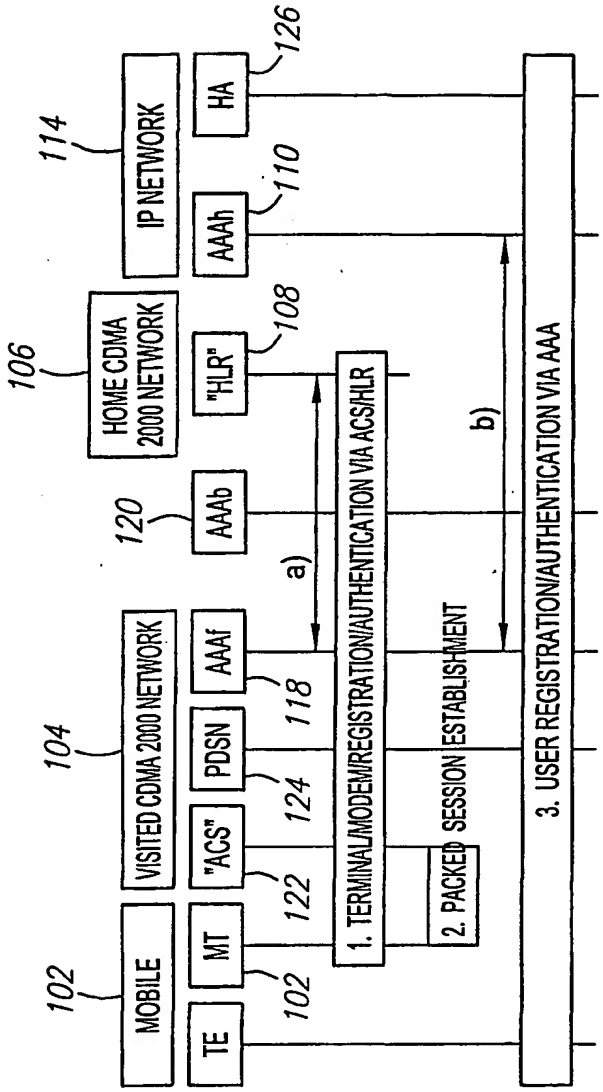

MOBILE
TE
MT
VISITED CDMA 2000 NETWORK
"ACS"
PDSN
AAAf
HOME CDMA 2000 NETWORK
AAAb
"HLR"
IP NETWORK
AAAh
HA
102
102
104
122
124
118
120
106
108
114
110
126
a)
b)
1. TERMINAL/MODEM/REGISTRATION/AUTHENTICATION VIA ACS/HLR
2. PACKED SESSION ESTABLISHMENT
3. USER REGISTRATION/AUTHENTICATION VIA AAA

FIG. 2

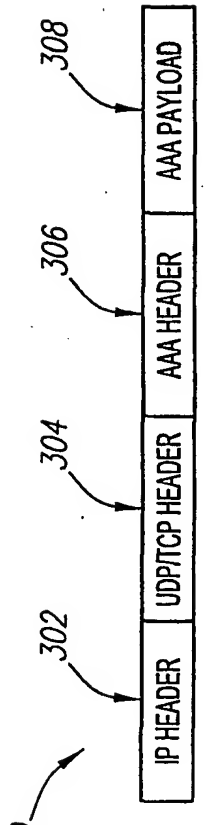

IP HEADER
UDP/TCP HEADER
AAA HEADER
AAA PAYLOAD
300
302
304
306
308

FIG. 3